OBJECTIVES

CHAPTER 3

Configuring, Managing Monitoring, an Troubleshooting Remot Access in a Windows 200 Network Infrastructur

If you have ever used a modem to connect your Windows computer to another server or network, you have used remote access. With Windows 2000, Microsoft has introduced many new remote access capabilities to its operating system. This chapter covers the "Configuring, Managing, Monitoring, and Troubleshooting Remote Access in a Windows 2000 Network Infrastructure" objectives for this exam. As today's workforce becomes more and more diverse, the ability to provide reliable and secure remote access is becoming critical in every environment.

Microsoft defines the "Configuring, Managing, Monitoring, and Troubleshooting Remote Access in a Windows 2000 Network Infrastructure" objectives as

Configure and troubleshoot remote access.

- **Configure inbound connections.**
- **Create a remote access policy.**
- **Configure a remote access profile.**
- **Configure a virtual private network (VPN).**
- **Configure multilink connections.**
- **Configure Routing and Remote Access for DHCP Integration.**

▶ One of the functions that Windows servers have always had is as a remote access server. With Windows 2000, Microsoft enhances your remote access capabilities. This objective expects you to understand how to configure the different remote access features included with Windows 2000 Server.

Manage and monitor remote access.

▶ If you are going to use your Windows 2000 server for remote access, you need to know how to manage and monitor it. This objective tests your understanding of remote access management and monitoring.

OBJECTIVES

Configure remote access security.

- **Configure authentication protocols.**
- **Configure encryption protocols.**
- **Create a remote access policy.**

▶ Security is becoming more important in today's computing environment. This objective tests your understanding of the security capabilities of Windows 2000 Server and remote access.

OUTLINE

Configuring and Troubleshooting Remote Access 132

Understanding Remote Access Protocols 134
Configuring Inbound Connections 135
Creating a Remote Access Policy 139
Configuring a Remote Access Profile 143
Configuring a Virtual Private Network (VPN) 147
Configuring Multilink Connections 151
Configuring Routing and Remote Access for DHCP Integration 151

Managing and Monitoring Remote Access 152

Configuring Remote Access Security 156

Configuring Authentication Protocols 158
Configuring Encryption Protocols 159

Chapter Summary 163

Apply Your Knowledge 164

STUDY STRATEGIES

- Be sure you have a thorough understanding of the security capabilities of all the different remote access mechanisms. With the focus on security in the industry today, Microsoft considers security to be one of the cornerstones of Windows 2000.
- Review the different types of encryption available for authenticating and securing your information through remote access.
- Pay close attention to the capabilities of remote access policies. Windows 2000 includes a number of policy-based management capabilities, and understanding the policies associated with remote access is important for this exam.
- Be sure to complete the exercises at the end of the chapter. Microsoft is striving to make certification exams more rigorous. Familiarity not only with the theory, but also with the hands-on portion of the configuration and troubleshooting of remote access is important for this exam.

06W2000 NITG-03 10/11/00 12:59 PM Page 132

CONFIGURING AND TROUBLESHOOTING REMOTE ACCESS

Configure and troubleshoot remote access.

Before we begin discussing how to configure remote access with Windows 2000 Server, we should take a minute to review what exactly remote access is under Windows 2000. If you have worked with Windows NT 4, you are undoubtedly familiar with the Remote Access Service (RAS). RAS was an NT 4 add-on service, which provided the capability to receive incoming modem calls and allowed the user to connect to the network. RAS was also used for the other direction: you needed RAS to connect your Windows NT server or workstation to another host, either NT or a generic dial-in server.

This model has changed dramatically in Windows 2000. Not only is the Routing and Remote Access Service (the next generation of the Remote Access Service) installed automatically with the operating system, it also bundles a number of features that used to be distributed through other services under Windows NT. For example, not only are RAS services available with Routing and Remote Access, but the Windows 2000 VPN service is included in Routing and Remote Access, as well.

But before you jump into configuring the Routing and Remote Access Service, let's discuss some of the reasons for deploying remote access and some of the specifics surrounding the Windows 2000 Routing and Remote Access.

Microsoft has included remote access capabilities in all its operating systems since the introduction of Windows for Workgroups (a remote access client computer) and the Windows NT Advanced Server (a remote access server). If you have worked with earlier versions of Windows NT or Windows 9x, you are probably familiar with the term RAS, first used to discuss the NT Remote Access Server and later used as a generic description of most of the Windows operating system remote access applications. This changed in the midst of the Windows NT Server 4 operating system's life cycle, with the introduction of an add-on service upgrade known as the Routing and Remote Access Service, which you should note carried over to the Windows 2000 operating system. The main reason for the change is that Microsoft needed to enhance its offerings

06W2000 NITG-03 10/11/00 12:59 PM Page 133

in the remote access and routing areas of networking. The Routing and Remote Access upgrade provided the first framework for integrating all network services into a single application. Routing and Remote Access introduced the following features to Windows NT networking:

- A unified service for Routing and Remote Access integrated with the operating system.
- A full set of routing protocols for IP and IPX (including the noteworthy addition of OSPF).
- APIs for third-party routing protocols, user interface, and management.
- Demand-dial routing.
- PPTP server-to-server for secure VPNs.
- Remote Authentication Dial-In User Service (RADIUS) client support.

But enough history. Let's look at what the Routing and Remote Access Service included with Windows 2000 brings to the table. Routing and Remote Access includes the following capabilities:

- Full integration into the Windows 2000 operating system. This is not an add-on or a patch, but a fully integrated service built from the ground up as part of Windows 2000.
- Consistent management interface for all routing-based activities, including remote access, VPN, and IP and IPX routing.
- Fewer reboots. If you worked with earlier versions of Windows, you are familiar with the "change any network configuration and reboot the machine" method of managing Windows networking. With Windows 2000, the number of times you need to reboot the server is dramatically lessened. Although you may still need to reboot occasionally, most activities can be done without impacting operations.
- Additional VPN services and simplified VPN management. The VPN interfaces (PPTP and L2TP) are installed and configured by default, requiring no additional configuration. There is also support for the IPSec protocol.

06W2000 NITG-03 10/11/00 12:59 PM Page 134

EXAM TIP

Authentication Support Only Windows 2000 Server supports EAP and RADIUS for authentication.

- Network Address Translation (NAT) has been added, as has Internet Connection Sharing (ICS).
- Additional authentication mechanisms have been added to Routing and Remote Access, including MS-CHAP v2, RADIUS, and EAP (for smart card and certificate support).

One other key point to remember when discussing Microsoft's Routing and Remote Access Service and the remote access capabilities is that in previous incarnations, the term RAS, or Remote Access Service, was used interchangeably to refer to the dial-in connections and the service that ran the dial-up server. With the new Routing and Remote Access Service, Microsoft is striving to clarify its use of terminology. So in Windows 2000 parlance, Routing and Remote Access refers only to the Routing and Remote Access application. The server is called either a dial-in or dial-up server, or in the case of VPN, a VPN server. The client computers are called dial-in or dial-up clients.

It is important to keep in mind that Microsoft's Routing and Remote Access Service considers all connections to be LAN connections. What this means from a functionality perspective is that all the services that are available via LAN connection are also available via a modem connection.

Understanding Remote Access Protocols

Microsoft's Routing and Remote Access Service supports two data link control protocols for asynchronous connections:

- **Serial Line Interface Protocol (SLIP).** The granddaddy of serial line protocols, SLIP is supported for legacy applications and is almost never used.
- **Point-to-Point Protocol (PPP).** PPP is the protocol most of us use when connecting via modem. PPP can automatically establish and re-establish connections; it uses error correction, and it can support multiple protocols. The Windows 2000 implementation for PPP is fully RFC 1661 "Point-to-Point Protocol" compliant.

06W2000 NITG-03 10/11/00 12:59 PM Page 135

Windows 2000 can connect to any other RFC 1661-compliant dial-up server and can accept connections from any compliant client computers. The real strength of this protocol is the support for multiple network protocols, such as IPX, IP, and AppleTalk. SLIP was restricted to IP only. PPP also uses a number of authentication protocols, discussed later in the chapter.

We will discuss many of these features as we move through this chapter. For now, let's take a look at the simplest use for the Routing and Remote Access Service.

Configuring Inbound Connections

If you have mobile users, it is a safe bet that you have dealt with requests for access to the network. This could be for access to mail, the company intranet, or even to file shares or applications. Windows 2000 includes as part of Routing and Remote Access the capability to permit inbound connections via attached modems.

EXAM TIP

Support for Inbound Dial-In Connections Windows 2000 Server supports 256 inbound dial-in connections. Windows 2000 Professional supports 1.

IN THE FIELD

ISSUES TO CONSIDER IN CONFIGURING SYSTEMS FOR MOBILE USERS

If you deploy Windows 2000 as your remote access solution for mobile users, you will need to keep a couple of things in mind. First, because any server has only a limited number of communication ports, you will probably need a multiport modem card. Various manufacturers offer these types of products, but be sure to check the Microsoft Hardware Compatibility List before making any purchases.

You should also avoid installing this capability on any domain controllers or application servers. Although the overhead associated with supporting dial-in users is fairly low, the security ramifications of connecting a modem or modems to a production application server, or even worse—a domain controller, are significant. You should try to avoid that architecture if at all possible.

In the latest version of Routing and Remote Access, Microsoft has added some new features as part of the management. One of the features that has the most impact on the discussion of remote access is the addition of remote access policies. Remote access

continues

06W2000 NITG-03 10/11/00 12:59 PM Page 136

continued

policies are a radical departure from the Windows NT 3.5x and 4 models, in which user authorization was based on a simple Grant Dial-In Permission to User option in User Manager or the Remote Access Admin console. Callback options were also configured on a per-user basis. In Windows 2000, authorization is granted based on the dial-in properties of a user account and remote access policies.

Remote access policies are a set of conditions and connection settings that give network administrators more flexibility in authorizing connection attempts. The Windows 2000 Routing and Remote Access Service uses remote access policies to determine whether to accept or reject connection attempts. With remote access policies, you can grant remote access by individual user account or through the configuration of specific remote access policies. We look at setting up a policy in the "Creating a Remote Access Policy" section later in the chapter.

Windows 2000 uses three types of policies to control remote access:

- **Local Internet Authentication Services policies**. These local policies are derived from RADIUS and can be used to define access permissions based on a number of client attributes.
- **Central Internet Authentication Services policies**. A dial-up server can be configured to use a central IAS RADIUS server to provide its policies. This allows multiple Routing and Remote Access dial-up servers to use the same policies without requiring the manual replication of policies and settings.
- **Group Policies.** More in line with the older versions of remote access. Access can be controlled by group policies.

EXAM TIP

Be Familiar with IAS Internet Authentication Services (IAS) are the new RADIUS authentication capabilities included with Windows 2000. They are used heavily in conjunction with Routing and Remote Access policies.

EXAM TIP

Know Where Remote Access Group Policies Are Stored They're stored in the file system in the default WINNT\SYSVOL\SYSVOL\<domain name> directory.

EXAM TIP

Remember to Use the Snap-in If you are configuring Routing and Remote Access for dial-up access on a domain controller, you must use the Routing and Remote Access snap-in.

Now let's look at how to configure a Windows 2000 server to support an inbound connection.

STEP BY STEP

3.1 Configuring Remote Access Inbound Connections

1. Right-click the My Network Places icon on the desktop. From the Context menu, select Properties. The Network and Dial-up Connections window opens. (You can also open this window by going to Start, Settings, Network and Dial-up Connections).

06W2000 NITG-03 10/11/00 12:59 PM Page 137

2. Double-click the Make New Connection icon. The Network Connection Wizard starts. If you have not already configured your dialing location information (see Figure 3.1) you will be prompted to do so before continuing with the wizard. Fill in the information and click OK. You will see the new location entry in the Phone and Modem Options window. Click OK to close it and return to the wizard.

3. Click Next to start the wizard process. The Network Connection Type dialog box opens (see Figure 3.2). Select the Accept Incoming Connections option and click Next. The Devices for Incoming Connections dialog box (see Figure 3.3) opens.

continues

Location Information
Before you can make any phone or modem connections, Windows needs the following information about your current location.
What country/region are you in now?
United States of America
What area code (or city code) are you in now?
If you dial a number to access an outside line, what is it?
The phone system at this location uses:
Tone dialing
Pulse dialing
OK
Cancel

FIGURE 3.1
The Location Information is needed so that the server knows whether a call is local or long distance. In the case of a dial-in server, this is needed for callbacks.

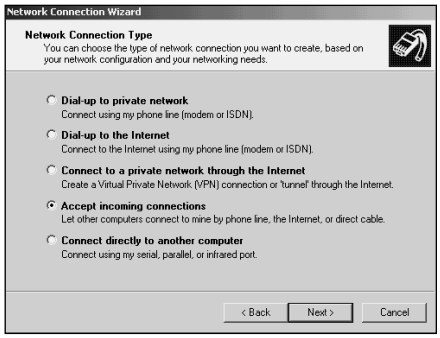
Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

FIGURE 3.2
The Network Connection Type dialog box allows you to select from a variety of Routing and Remote Access connection options.

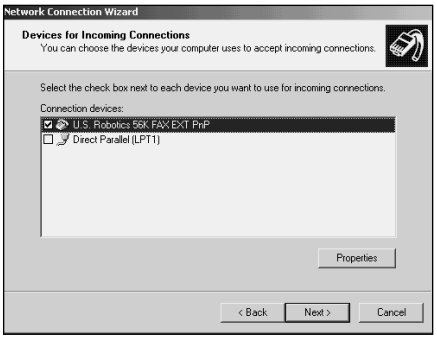
Network Connection Wizard
Devices for Incoming Connections
You can choose the devices your computer uses to accept incoming connections.
Select the check box next to each device you want to use for incoming connections.
Connection devices:
U.S. Robotics 56K FAX EXT PnP
Direct Parallel (LPT1)
Properties
< Back
Next >
Cancel

FIGURE 3.3
This dialog box allows you to selectively enable the devices that will be accepting incoming calls.

06W2000 NITG-03 10/11/00 12:59 PM Page 138

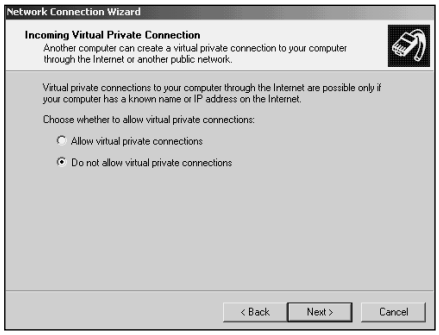
Network Connection Wizard
Incoming Virtual Private Connection
Another computer can create a virtual private connection to your computer through the Internet or another public network.
Virtual private connections to your computer through the Internet are possible only if your computer has a known name or IP address on the Internet.
Choose whether to allow virtual private connections:
Allow virtual private connections
Do not allow virtual private connections
< Back
Next >
Cancel

FIGURE 3.4
In addition to supporting inbound modem connections, Windows 2000 also has the capability to accept inbound virtual private connections.

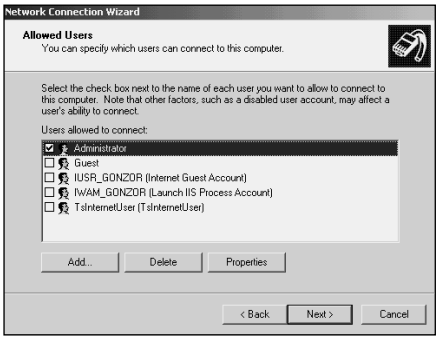
Network Connection Wizard
Allowed Users
You can specify which users can connect to this computer.
Select the check box next to the name of each user you want to allow to connect to this computer. Note that other factors, such as a disabled user account, may affect a user's ability to connect.
Users allowed to connect:
Administrator
Guest
IUSR_GONZOR (Internet Guest Account)
IWAM_GONZOR (Launch IIS Process Account)
TsInternetUser (TsInternetUser)
Add...
Delete
Properties
< Back
Next >
Cancel

FIGURE 3.5
You can select the users who should be able to connect. However, if their account is disabled or locked, they will not be able to connect.

continued

4. Select the device(s) that you want to receive the incoming calls and click Next. The Incoming Virtual Private Connection dialog box opens (see Figure 3.4).

5. Because we will discuss creating a virtual private network (VPN) connection in the "Configuring a Virtual Private Network (VPN)" section of this chapter, select Do Not Allow Virtual Private Connections and click Next. The Allowed Users dialog box opens (see Figure 3.5).

6. Select the users you want to have dial-in access. Click Properties to open the user properties. This allows you to configure callback, if necessary.

7. Click the Callback tab (see Figure 3.6). For the most secure access, select Always Use the Following Callback Number and enter the user's phone number. Click OK to return to the wizard, and click Next to continue. The Networking Components dialog box opens (see Figure 3.7).

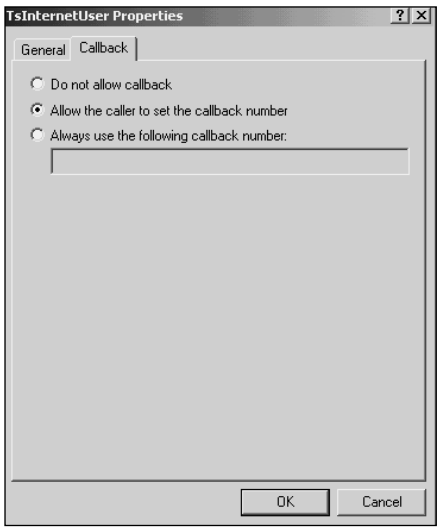

FIGURE 3.6
In a highly secure environment, use of the callback options included with Windows 2000 is a necessity.

06W2000 NITG-03 10/11/00 12:59 PM Page 139

8. Select the components you want the dial-in user to have access to after they connect. By default, all components are selected. Click Next to continue. The Completing the Network Connection Wizard dialog box opens (see Figure 3.8).
9. Enter an intuitive name for the new connection and click Finish to complete the installation.

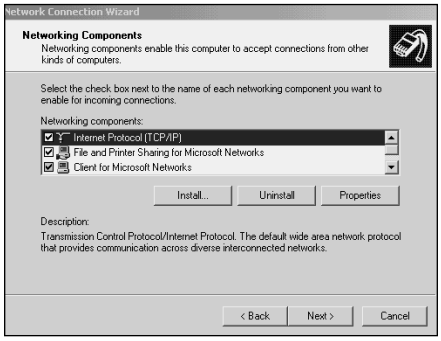
Network Connection Wizard
Networking Components
Networking components enable this computer to accept connections from other kinds of computers.
Select the check box next to the name of each networking component you want to enable for incoming connections.
Networking components:
Internet Protocol (TCP/IP)
File and Printer Sharing for Microsoft Networks
Client for Microsoft Networks
Install...
Uninstall
Properties
Description:
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
< Back
Next >
Cancel

FIGURE 3.7
The Networking Connections dialog box determines which services are available to dial-in users.

Now that you have a dial-up connection, let's take a look at creating a remote access policy to define what can be done with the new connections.

Creating a Remote Access Policy

A remote access policy is a set of actions that can be applied to a group of users that meet a specified set of requirements. The example Microsoft uses to illustrate this point is to think about email rules. In many email packages, you can configure a rule that allows you to delete all messages from a specific user or group of users. A remote access policy is similar in that you can specify actions based on a number of criteria. To illustrate how this works, let's run through creating a remote access policy.

Network Connection Wizard
Completing the Network Connection Wizard
The connection will be named:
Incoming Connections
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
< Back
Finish
Cancel

FIGURE 3.8
This dialog box allows you to enter a descriptive name for the new connection.

06W2000 NITG-03 10/11/00 12:59 PM Page 140

STEP BY STEP

3.2 Creating a Remote Access Policy

1. Open the Routing and Remote Access console by going to Start, Programs, Administrative Tools, Routing and Remote Access (see Figure 3.9).
2. Expand the application tree in the left pane by double-clicking the server. Right-click Remote Access Policies and select New Remote Access Policy. The Add Remote Access Policy window opens (see Figure 3.10).

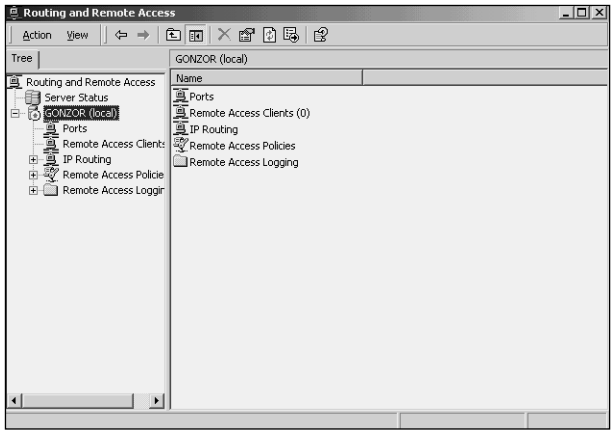

FIGURE 3.9
The Routing and Remote Access console allows you to manage your remote access server, including creating remote access policies.

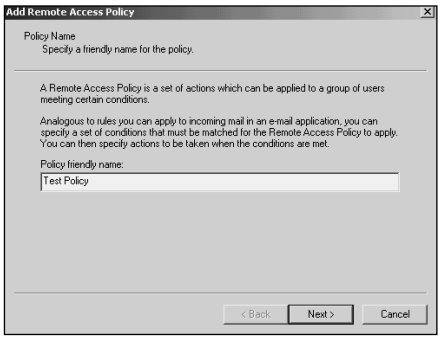
Add Remote Access Policy
Policy Name
Specify a friendly name for the policy.
A Remote Access Policy is a set of actions which can be applied to a group of users meeting certain conditions.
Analogous to rules you can apply to incoming mail in an e-mail application, you can specify a set of conditions that must be matched for the Remote Access Policy to apply. You can then specify actions to be taken when the conditions are met.
Policy friendly name:
Test Policy
< Back
Next >
Cancel

FIGURE 3.10
This dialog box allows you to give your policy a user-friendly name.

06W2000 NITG-03 10/11/00 12:59 PM Page 141

3. Enter a user friendly name and click Next to continue. The Add Remote Access Policy Conditions dialog box opens (see Figure 3.11).

4. Click Add to add a condition. Select one attribute from the list of attributes (shown in Figure 3.12). Each attribute will create a slightly different process, and you will need to configure the attribute appropriately. For this example, select Windows-Groups. Using the Windows-Groups attribute allows you to enable remote access by user groups, as defined in the Users and Groups console.

5. Click Add to go to the Groups dialog box (see Figure 3.13). Then click Add to open the Select Groups dialog box

continues

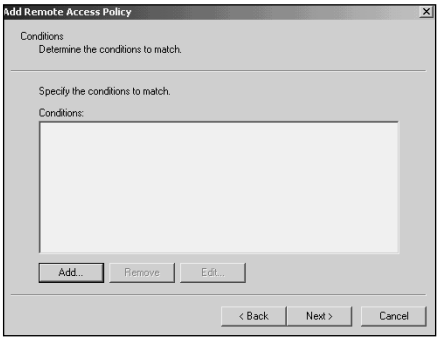

FIGURE 3.11
The first step in creating a remote access policy is to set the conditions.

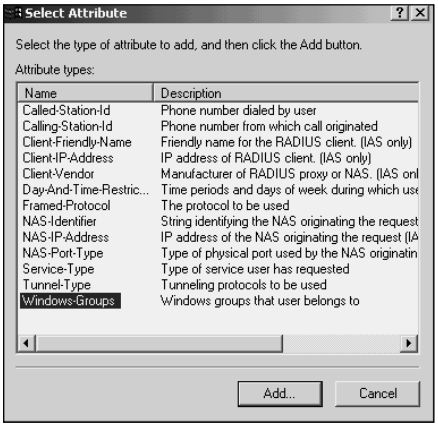

FIGURE 3.12
Select the appropriate attributes for the policy you are trying to create.

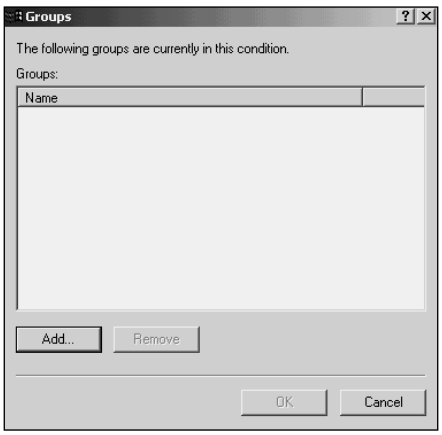

FIGURE 3.13
As a general rule, Windows-Groups is an attribute that is used frequently with remote access policies because it allows you to intuitively group users by department, function, or access rights.

06W2000 NITG-03 10/11/00 12:59 PM Page 142

continued

shown in Figure 3.14 and select the appropriate group(s) for the rule. Click OK to return to the Groups dialog box. Click OK to add the Windows-Groups condition to the policy. If you were to add an additional condition, users would need to meet both conditions to have the policy applied (a logical AND operation).

6. Click Next to open the Add Remote Access Policy permissions dialog box shown in Figure 3.15. You can either Grant or Deny Remote Access Permission by selecting the appropriate option. Select the Deny Remote Access Permission option and click Next. The Edit Dial-in Profile dialog box that opens allows you to access the dial-in

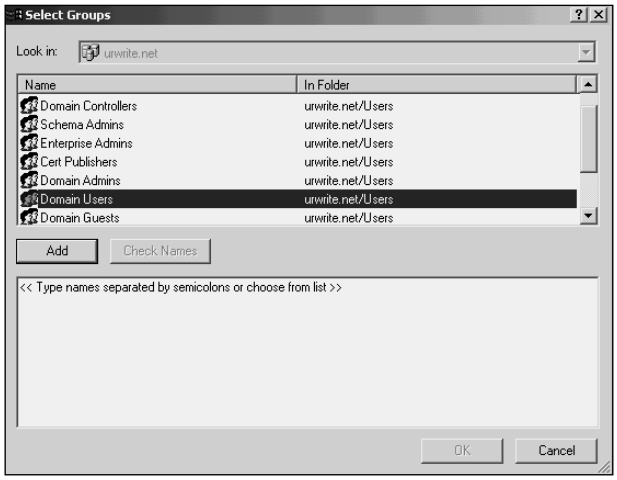

FIGURE 3.14
Select the appropriate groups for remote access permissions.

Add Remote Access Policy
Permissions
Determine whether to grant or deny remote access permission.
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.
If a user matches the specified conditions:
Grant remote access permission
Deny remote access permission
< Back
Next >
Cancel

FIGURE 3.15
You can grant or deny permissions from this screen.

06W2000 NITG-03 10/11/00 12:59 PM Page 143

profile for the users affected by this policy (see Figure 3.16). You can restrict a number of access parameters, which we discuss at the end of the section.

7. Click OK to return to the User Profile screen.
8. Click Finish to complete the creation of the profile.

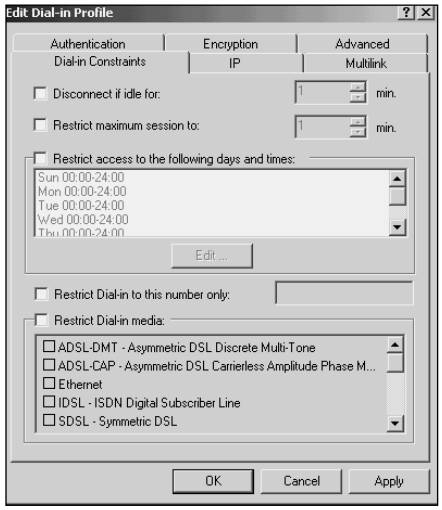

FIGURE 3.16
The Edit Dial-in Profile dialog box allows you access to the granular settings for the dial-in users.

IN THE FIELD

DESIGN YOUR POLICIES WITH CARE

One thing you will find if you work in a large remote access environment is the uses for group-based policies. A couple of places these types of groups can be very useful include creating a group for contractors who work for your company intermittently. You can create an allow access and a deny access group, and then depending on the status of any projects, you can control their access to remote access just by moving their account from one group to another. People on a leave of absence might be placed in an LOA group to block them from remote access until they come back on the job. The variations are endless. The trick is to really put some thought into the policy design before you start creating users. If you just start creating users with the thought of going back and organizing later, you have probably created three times as much work for yourself.

Configuring a Remote Access Profile

Now that you understand how to create a remote access policy, we need to discuss the next phase of the process—configuring a remote access profile. To configure a remote access profile, follow the steps in Step by Step 3.3.

06W2000 NITG-03 10/11/00 12:59 PM Page 144

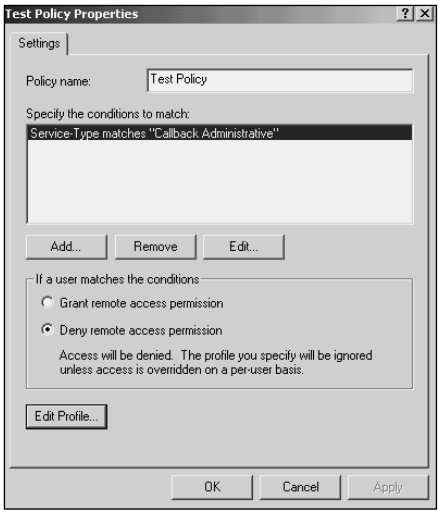

FIGURE 3.17
The Policy Properties dialog box contains all the information regarding the policy.

STEP BY STEP

3.3 Configuring a Remote Access Profile

1. Open the Routing and Remote Access console by going to Start, Programs, Administrative Tools, Routing and Remote Access.
2. Right-click the remote access policy you want to configure the remote access profile for. Select Properties from the Context menu. The Policy Properties dialog box opens (see Figure 3.17). The name in the title bar reflects the name of the policy.
3. Click the Edit Profile button. The Edit Dial-in Profile dialog box opens (refer to Figure 3.16).
4. Make any modifications necessary and click OK to return to the Properties dialog box. Click OK again to commit the changes and return to the OS.

That's how you get to the parameters for the profile. Now let's take a look at some of the parameters you can configure before we move on to VPNs in the next section.

The dial-in profile contains the following settings:

- **Dial-in Constraints.** This tab (refer to Figure 3.16) allows you to configure the restrictions on the dial-in users, including the idle disconnect timer, the maximum length of the session, the time and day access is permitted, the dial-in number allowed, and the dial-in media allowed.

NOTE

What Is Dial-in Media? This is more applicable with a VPN connection than a dial-in connection, but you have the ability to disallow specific network media from connecting to the server. For example, if you didn't want ADSL users to be able to connect, you can specifically deny it.

06W2000 NITG-03 10/11/00 12:59 PM Page 145

- **IP.** This tab (shown in Figure 3.18) is used to determine the IP Address Assignment Policy, if necessary. The following are three possible settings for the IP Address Assignment Policy:
  - **Server Must Supply an IP Address.** For this to work, the server must have a DHCP range configured for remote access. The client computer cannot connect without requesting an address.
  - **Client May Request an IP Address.** This setting leaves the determination on whether to use a DHCP address to the client computer. If the client computer has a statically configured address, it will still be able to connect.
  - **Server Settings Define Policy.** This setting defers the decision on IP address policy to the Routing and Remote Access Server's global policy.

  You can also apply IP Packet Filters from the IP tab. Packet filters can be configured for traffic sent to the client computer or traffic received from the client computer. These filters are applied by network and can be used to filter a variety of IP-based protocols, including Any, Other, ICMP, UDP, TCP, and TCP [established].

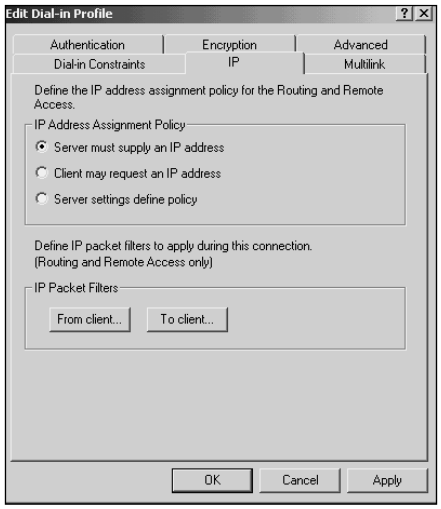

FIGURE 3.18
The IP tab can be used to set IP filters on a policy.

- **Multilink.** This tab (see Figure 3.19) allows you to configure Windows 2000's capability to aggregate multiple analog phone lines connected to multiple modems to provide greater bandwidth. The Multilink Settings section allows you to configure the following:
  - **Default to Server Settings.** Defers the configuration to the Routing and Remote Access global settings.
  - **Disable Multilink (Restrict Client to a Single Port).** This setting is self-explanatory.
  - **Allow Multilink.** This configuration allows a client computer to connect using multiple ports, and you can configure the number of ports they can use.

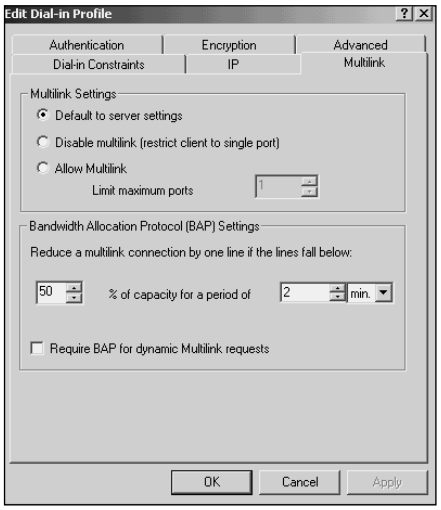

FIGURE 3.19
The multilink capabilities of Windows 2000 allow you to maximize bandwidth across multiple analog phone systems.

06W2000 NITG-03 10/11/00 12:59 PM Page 146

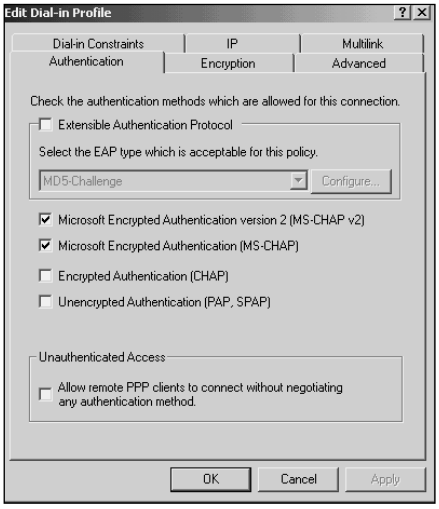

FIGURE 3.20
To take advantage of the multilink capabilities of Windows 2000, you need to enable it here for the appropriate group.

The Bandwidth Allocation Protocol (BAP) Settings can be used to configure when to drop one of the multilink lines, based on usage. If the usage drops below a configurable amount of bandwidth (50% is the default) for a specified amount of time (2 minutes is the default), one of the multilink lines is dropped. You can also enable the Require BAP for Dynamic Multilink Requests.

- **Authentication.** This tab (see Figure 3.20) allows you to configure the authentication methods supported by Windows 2000. (The protocols listed in the figure are discussed later in this chapter.)
- **Encryption.** This tab (see Figure 3.21) allows you to set the level of encryption required with Routing and Remote Access authentication. You can set it to No Encryption, Basic, or Strong, or allow any combination of the three.
- **Advanced.** The Advanced tab (see Figure 3.22) allows you to add connection attributes to be returned to the Remote Access Server. This is usually used in conjunction with RADIUS.

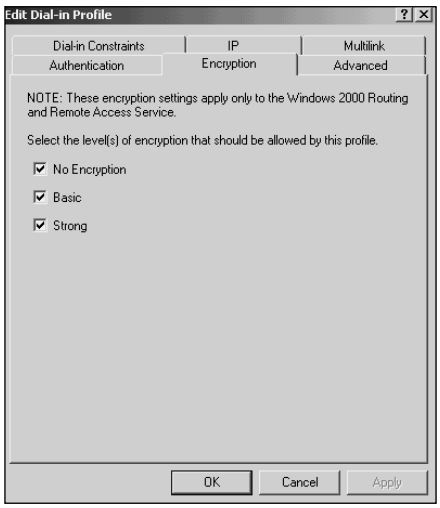

FIGURE 3.21
Routing and Remote Access supports three levels of encryption.

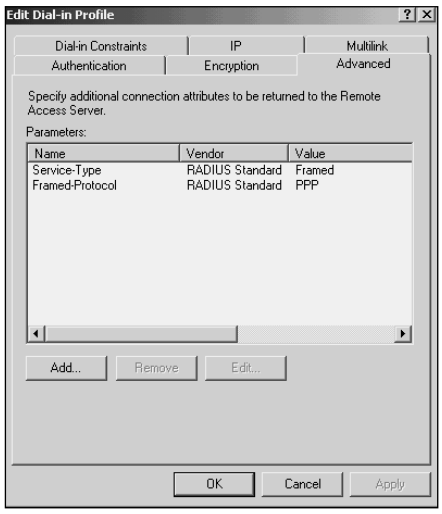

FIGURE 3.22
If you need to configure RADIUS attributes, use this tab.

06W2000 NITG-03 10/11/00 12:59 PM Page 147

IN THE FIELD

PUTTING RADIUS TO WORK

If you have worked in a large remote access environment, you might have run across RADIUS already. But for those of you who haven't, we will discuss it a bit here. RADIUS (Remote Authentication Dial-in User Service) is an authentication and accounting system used by many Internet Service Providers (ISPs) and enterprise networks. When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct and then authorizes access to the ISP system. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Another place you see RADIUS used is to leverage the account information in a Windows 2000 domain. The built-in RADIUS server can be used not only to authenticate Routing and Remote Access client computers, but it can also be used by third-party dial-in servers as an authentication method. In fact, some ISPs authenticate users for an enterprise account by passing RADIUS authentication requests to a local RADIUS server, allowing the company to control who gets access to the Internet.

Configuring a Virtual Private Network (VPN)

Before we delve into configuring the Windows 2000 VPN, let's look at VPNs in general and some of the factors that led to the creation of them. If you have been around the industry for a while, you are probably aware that one of the most misused terms in the computer industry today is VPN. It seems as though every vendor has a VPN to sell you, and many times one vendor's VPN can seem to be the exact opposite of another's. For example, not too long ago, one of the major telecommunications vendors offered a VPN service that consisted of a private frame-relay network that users could dial in to, and then utilizing the frame relay network, connect to the business's

06W2000 NITG-03 10/11/00 12:59 PM Page 148

network. This service involved no encryption, and the only true security provided by the solution was whatever mechanism the customer provided at the frame relay's point of entry to the corporate network. Another VPN vendor will try to sell you a dedicated hardware platform designed to provide strictly VPN services. Firewall vendors will try to sell you VPN in their firewall platform, and router vendors will try to convince you that the VPN services bundled with your router are the solution for you. Finally, there are the solutions that run on a network operating system, such as the VPN bundled with Windows 2000. For the sake of our discussion, a VPN is a private network that is constructed using a public network (such as the Internet) to connect its nodes.

The first thing you need to be aware of when discussing the Windows 2000 VPN is the encryption protocols available. Windows 2000 has two main encryption protocols that are used in the VPN. They include

- **Point-to-Point Tunneling Protocol (PPTP).** PPTP is Microsoft's legacy protocol for supporting VPNs. Developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known collectively as the PPTP Forum, PPTP encountered some security issues in its original form. It has been revised by Microsoft but has never been widely accepted by the security community. Although still supported on a variety of vendors' VPN servers, PPTP is rapidly being overtaken by the more widely adopted IPSec protocol.
- **IP Security Protocol (IPSec).** IPSec is a suite of cryptography-based protection services and security protocols that are used for the first standards-based VPN protocol. In Windows 2000, IPSec is used to provide machine-level authentication, as well as data encryption, for L2TP-based (Layer 2 Tunneling Protocol) VPN connections. Unlike some other IPSec-based VPNs, Microsoft's implementation uses the L2TP protocol for encrypting the usernames, passwords, and data, whereas IPSec is used to negotiate the secure connection between your computer and its remote tunnel server.

06W2000 NITG-03 10/11/00 12:59 PM Page 149

TABLE 3.1

THE DIFFERENCES BETWEEN L2TP/IPSEC AND PPTP

L2TP/IPSec	*PPTP*
Standards-based	Microsoft proprietary
Windows, Linux, Macintosh, Solaris, and other platforms	Windows OS and Linux platforms
DES / 3DES encryption	Microsoft proprietary encryption
Requires only that the tunnel media provide packet-oriented point-to-point connectivity	Requires an IP-based transit internetwork
Supports header compression	No header compression

EXAM TIP

Know the Differences Between L2TP and PPTP Because Microsoft uses a custom protocol configuration for its IPSec VPN implementation, you should be sure that you understand the differences between IPSec and PPTP, as well as how Microsoft implemented its version of IPSec. Table 3.1 can help you keep them straight.

Now that you know what a VPN is and how it works, let's set up one. The good news is that installing Routing and Remote Access automatically makes a VPN connection available. What you need to understand at this point is how to configure the VPN that is installed. To configure the VPN service, do the following:

STEP BY STEP

3.4 Configuring a Virtual Private Network

1. Open the Routing and Remote Access by going to Start, Programs, Administrative Tools, Routing and Remote Access.
2. Click the Ports entry under the server. Notice that the sample configuration in Figure 3.23 shows five PPTP ports and five L2TP/IPSec ports. This is because the server had five user licenses configured when the Routing and Remote Access Service was installed.

continues

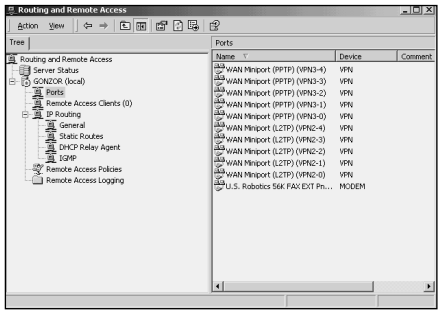

FIGURE 3.23
All the configured VPN ports will be displayed in the right window.

06W2000 NITG-03 10/11/00 12:59 PM Page 150

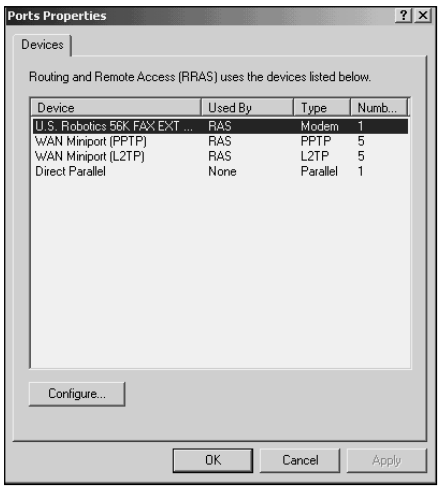

FIGURE 3.24
All the configured remote access connections appear here after they are installed.

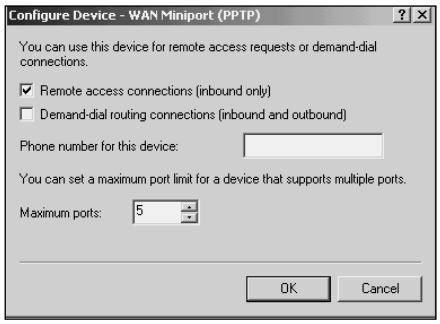
Configure Device - WAN Miniport (PPTP)
You can use this device for remote access requests or demand-dial connections.
Remote access connections (inbound only)
Demand-dial routing connections (inbound and outbound)
Phone number for this device:
You can set a maximum port limit for a device that supports multiple ports.
Maximum ports:
5
OK
Cancel

FIGURE 3.25
The Configure Device dialog box allows you to fine-tune the properties for the device, including the number of ports available.

continued

3. To configure the ports, select Ports in the left pane and right-click. From the Context menu select Properties. The Ports Properties dialog box opens (see Figure 3.24). You can see each of the protocols listed.
4. Select the protocol you want to modify and click Configure. The Configure Device dialog box (see Figure 3.25) opens. This screen allows you to set the direction of the interface (Inbound Only or Inbound and Outbound) as well as the number of ports. You can also set the phone number of the device, although this is of limited use with a VPN implementation.

That is all there is to configuring the VPN server bundled with Windows 2000.

IN THE FIELD

YOUR VPN IS ONLY AS GOOD AS YOUR INTERNET CONNECTION

Although VPNs are being used frequently to replace more traditional remote access methods, such as dial-in, people overlook a couple of things when putting together a VPN. First, the assumption is that a VPN will be faster than dialing a remote access server. This is not necessarily true. You can have a bottleneck at your ISP connection, congestion issues on the Internet, or even server capacity issues on the VPN server itself. Make sure you set realistic expectations for your users regarding the capabilities of your new VPN. Second, just putting up a VPN does not mean that all your remote access problems are solved. You'll find that a host of new issues can quickly arise. How end users get access to the Internet, the size and capacity of the VPN server, even the available Internet bandwidth can place a quick bottleneck on the performance of your VPN.

06W2000 NITG-03 10/11/00 12:59 PM Page 151

Configuring Multilink Connections

First introduced as part of Windows 98, Windows 2000 includes the capability of aggregating multiple modem lines to form a single, higher-bandwidth connection to a remote access server. This is usually an Internet Service Provider connection, but it could also be to another Windows 2000 Server, perhaps at a different location. As part of this capability, you also have the ability to leverage the Bandwidth Allocation Protocol (BAP). BAP is a PPP control protocol that is used to dynamically add or remove additional links to a multilink connection.

To set up a multilink connection, you just need to open the Network and Dial-up Connections window, right-click the Incoming Connections icon, select Properties (see Figure 3.26), and then select Enable Multilink.

Multilink is now configured. If a user dials in with two modems, the server will now aggregate the connections and allow the user to use the additional bandwidth as needed.

NOTE

Before You Begin Configuring Multilink If you want to configure multilink, there are a couple of prerequisites. First, you must have at least two modems installed on the system. After all, it's tough to multilink a single modem. Second, you need to have an incoming remote access connection created. Use Step by Step 3.1 to complete this activity.

EXAM TIP

Know Where Multilink Is Enabled More important, you should understand what is needed for a multilink connection and what benefits multilink provides.

Configuring Routing and Remote Access for DHCP Integration

If you have users that are connecting to your Routing and Remote Access server, you will probably want to dynamically assign them a TCP/IP address on the network. The best way to do this is with DHCP, which will need to be configured.

DHCP and the Routing and Remote Access Service have an important relationship that you need to understand. When the remote access server is configured to use DHCP, the Routing and Remote Access Server uses the DHCP client component to obtain 10 IP addresses from a DHCP server. This could be on the network or on the same server as Routing and Remote Access Server. The remote access server uses the first IP address obtained from DHCP for the RAS interface, and subsequent addresses are allocated to TCP/IP-based remote access client computers as they connect. IP addresses freed because of remote access client computers disconnecting are reused. When all 10 addresses have been allocated, the process starts again with the DHCP client computer requesting an additional 10 addresses.

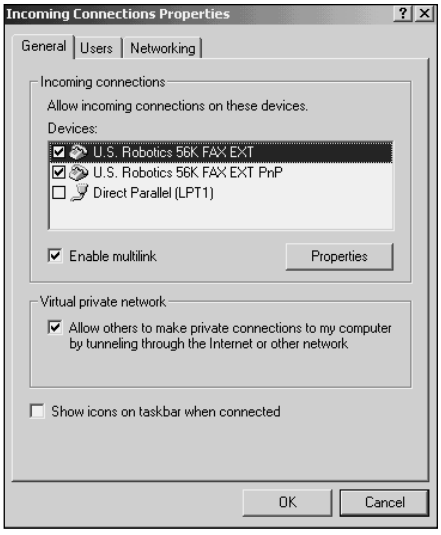

FIGURE 3.26
The Incoming Connections Properties dialog box allows you to configure all the parameters for dialing in, including the multilink configuration.

06W2000 NITG-03 10/11/00 12:59 PM Page 152

EXAM TIP

Know That Routing and Remote Access Service Requests Its DHCP Addresses 10 at a Time
When it exhausts its pool, it will go back to the DHCP server for an additional 10.

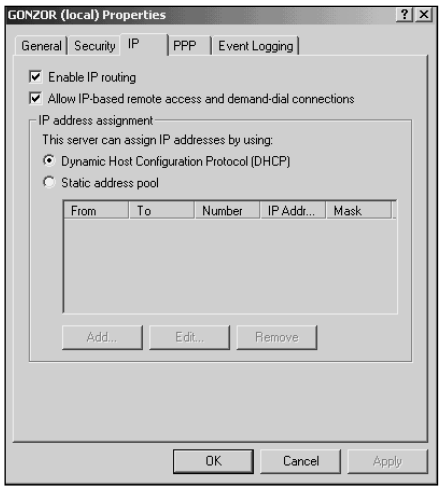

FIGURE 3.27
Configuring Routing and Remote Access to use DHCP is as easy as clicking an option.

EXAM TIP

Don't Memorize All the Counters
Just be familiar with the general categories and how to use the Performance console.

To configure Routing and Remote Access for DHCP integration, do the following:

STEP BY STEP

3.5 Configure Routing and Remote Access for DHCP Integration

1. Open the Routing and Remote Access console by going to Start, Programs, Administrative Tools, Routing and Remote Access.
2. From the tree, right-click the server and select Properties from the Context menu. Click the IP tab (see Figure 3.27).
3. In the IP address assignment section, click the Dynamic Host Configuration Protocol (DHCP).

Your Routing and Remote Access will now issue DHCP addresses for users connecting via dial-in or VPN.

MANAGING AND MONITORING REMOTE ACCESS

Manage and monitor remote access.

Now you have a functional Routing and Remote Access server up and running. How do you manage and monitor it? Let's start by taking a look at what kinds of information the Performance console can provide. It is generally the best tool for monitoring specifics about Windows 2000 services. The Performance console offers the following counters for the RAS object:

- **Alignment Errors.** The size of the packet received is different from the size expected.

06W2000 NITG-03 10/11/00 12:59 PM Page 153

- **Buffer Overrun Errors.** The software is unable to handle the rate that data is being received.
- **Bytes Received.** Total amount of bytes received by the service.
- **Bytes Received/Sec.** Number of bytes received by the service in a second.
- **Bytes Transmitted.** Total amount of bytes transmitted by the service.
- **Bytes Transmitted/Sec.** Number of bytes transmitted by the service in a second.
- **CRC Errors.** A frame received contains erroneous data and the packet did not pass the Cyclic Redundancy Check (CRC).
- **Frames Received.** Total number of frames received by the service.
- **Frames Received/Sec.** Number of frames received by the service per second.
- **Frames Transmitted.** Total number of frames transmitted by the service.
- **Frames Transmitted/Sec.** Number of frames transmitted by the service per second.
- **Percent Compression In.** Tells how well inbound traffic is being compressed.
- **Percent Compression Out.** Tells how well outbound traffic is being compressed.
- **Errors—Serial Overrun Errors, Timeout Errors, Total Errors, and Total Errors/Sec.** These objects handle all the error information for the Routing and Remote Access Service.

EXAM TIP

What Are We Measuring—Aggregate or Port Level? The Performance console allows you to monitor these counters on either a port–by–port or an entire server level. Select RAS Ports to look at a single port or RAS Total to see the stats for the entire server.

Now that we have looked at the counters for the service, let's take a look at some of the ways to monitor the service.

06W2000 NITG-03 10/11/00 12:59 PM Page 154

To configure Routing and Remote Access Performance monitoring, do the following:

STEP BY STEP

3.6 Monitor Routing and Remote Access

1. Open the Performance console by going to Programs, Administrative Tools, Performance (see Figure 3.28).
2. In Performance, select System Monitor.
3. To create an entry in System Monitor, click the Add (+) icon. The Add Counters window opens. By default, it opens to the Processor performance object.

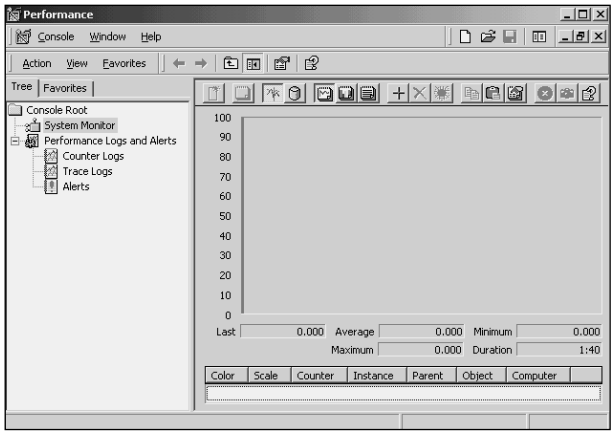

FIGURE 3.28
The Performance console allows you to monitor various system and application metrics for evaluating the performance and health of the system.

06W2000 NITG-03 10/11/00 12:59 PM Page 155

4. Select the RAS Port performance object. You will see the list of counters available for RAS displayed on the left and a list of RAS devices in the right pane (see Figure 3.29).
5. Select the port you want to monitor. After you have decided on the counter you want to monitor, click Add. You can add multiple counters either by selecting each counter and clicking Add, or by using the standard Windows multiple item select method of holding down the Ctrl key while you select all the counters you want to monitor, and clicking Add.
6. Click Close when you are done. You will see your counters being graphed similar to those shown in Figure 3.30.

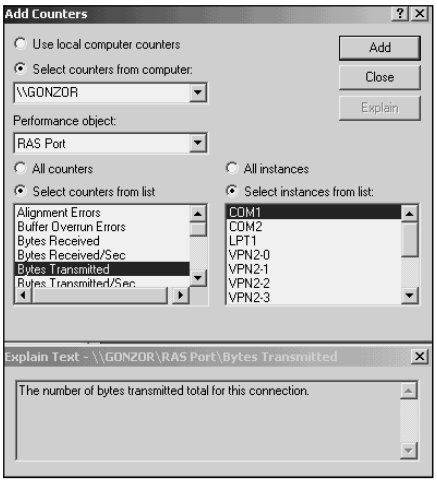

FIGURE 3.29
The counters associated with RAS are very similar to the errors offered for most LAN connections, including Ethernet.

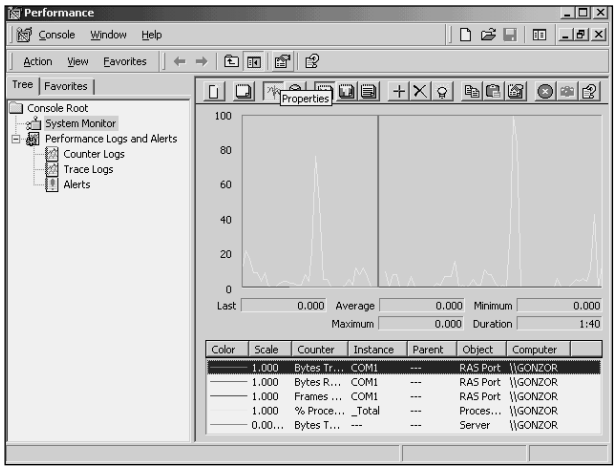

FIGURE 3.30
To find out what kinds of errors you may be experiencing in the field, keep an eye out for sudden jumps, either up or down. The graph in this figure shows that no RAS errors exist at this time.

06W2000 NITG-03 10/11/00 12:59 PM Page 156

If you want to see statistics on a VPN connection, do the following:

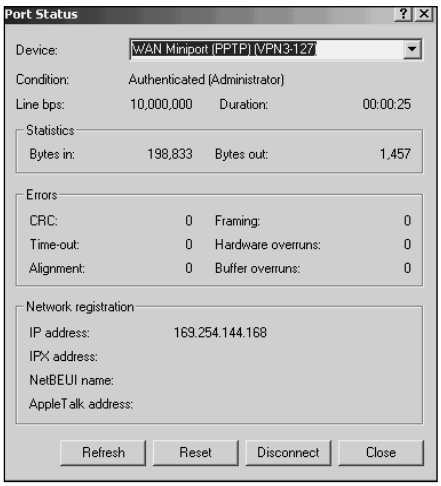

FIGURE 3.31
You can get a fairly complete port status here.

STEP BY STEP

3.7 Checking the Status of a Port

1. Open the Routing and Remote Access utility.
2. Select Ports in the left pane. A list of available ports appears in the right pane. Select the port you want to gather statistics from and right-click. From the Context menu, select Status. The Port Status dialog box opens (see Figure 3.31). You can see the port condition, the line speed, the call duration, network statistics, errors, and the network protocols being used, with addresses for the port.
3. You can reset or refresh the statistics by clicking the appropriate button at the bottom of the dialog box, and in the event someone is connected to the port, you can disconnect that connection by clicking Disconnect.

Now let's take a look at configuring remote access security.

CONFIGURING REMOTE ACCESS SECURITY

Configure remote access security.

The name of this section of the chapter is a bit of a misnomer. Most of what we have discussed in this chapter so far has to do with remote access security. But Microsoft has used the term Remote

06W2000 NITG-03 10/11/00 12:59 PM Page 157

Access Security for one specific group of settings. To configure this group of settings, do the following:

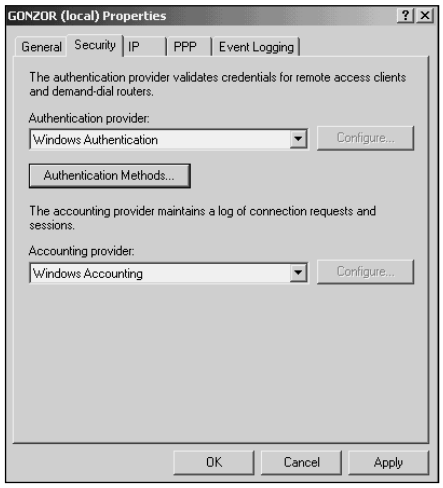

FIGURE 3.32
Remote Access security is controlled from this dialog box.

STEP BY STEP

3.8 Configuring Remote Access Security

1. Open the Routing and Remote Access console.
2. Right-click the server and select Properties. This opens the server properties.
3. Select the Security tab (see Figure 3.32). By default, the Authentication provider is Windows Authentication. You can also set it for RADIUS authentication. Select RADIUS from the pull-down menu.
4. Click Configure to configure the RADIUS server. The Edit RADIUS Server dialog box opens (see Figure 3.33). From here you can set the Name/Address of the RADIUS server, the shared secret, Timeout, Initial Score and RADIUS Port. You can also require the use of digital signatures.
5. Click OK to add the RADIUS server. Click OK to close the RADIUS Authentication dialog box. You will need to restart Routing and Remote Access to take advantage of the RADIUS authentication. Click OK to close the window.

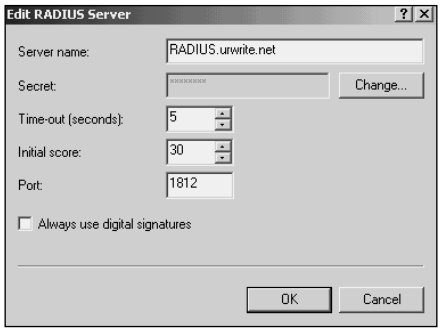

FIGURE 3.33
Adding a RADIUS server looks pretty easy, but you need to be sure your information matches the RADIUS server configuration.

Now that you have looked at how to do the RADIUS and Windows authentication, let's look at the authentication protocols Windows 2000 uses.

06W2000 NITG-03 10/11/00 12:59 PM Page 158

Configuring Authentication Protocols

Windows 2000 supports a number of authentication protocols; therefore, almost any connection configuration is supported. The protocols include the following:

- **Extensible Authentication Protocol (EAP).** EAP-TLS is an extension to the PPTP. EAP provides a standard mechanism for support of additional authentication methods within PPP, such as smart cards, one-time passwords, and certificates. EAP is critical for secure Windows 2000 VPNs because it offers stronger authentication methods (such as X.509 certificates) instead of relying on the user ID and password schemes used traditionally.
- **Challenge Handshake Authentication Protocol (CHAP).** CHAP negotiates an encrypted authentication using MD5 (Message Digest 5), an industry-standard hashing scheme. CHAP uses challenge-response with one-way MD5 hashing on the response. This allows you to authenticate to the server without actually sending your password over the network. Because this is an industry standard authentication method, it allows Windows 2000 to securely connect to almost all third-party PPP servers.
- **Microsoft-Created Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).** Microsoft created MS-CHAP, an extension of CHAP, to authenticate remote Windows workstations, increasing the protocol's functionality by integrating the encryption and hashing algorithms used on Windows networks. Like CHAP, MS-CHAP uses a challenge-response mechanism with one-way encryption on the response. Although MS-CHAP is consistent with standard CHAP as much as possible, the MS-CHAP response packet is in a format specifically designed for computers running a Windows operating system. A new version of the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP v2) is also available. This new protocol provides mutual authentication, stronger initial data-encryption keys, and different encryption keys for sending and receiving.

NOTE

MS-CHAP Versus MS-CHAP v2 Protocol When you are making a VPN connection, Windows 2000 Server attempts to authenticate using the MS-CHAP v2 protocol before offering the MS-CHAP protocol. If you are using an updated Windows client computer, you should be able to authenticate with the MS-CHAP v2 protocol. Windows NT 4 and Windows 98-based computers can use only MS-CHAP v2 authentication for VPN connections.

06W2000 NITG-03 10/11/00 12:59 PM Page 159

- **SPAP.** Shiva Password Authentication Protocol (SPAP) is used specifically to allow Shiva client computers to connect to a Windows 2000 Server and to allow Windows 2000 client computers to connect to Shiva servers.
- **PAP.** Password Authentication Protocol (PAP) uses unencrypted (plain text) passwords for authenticating users and is considered the least secure authentication protocol available. PAP is usually used as the authentication of last resort—used when a more secure form of authentication is not available. You might need to use this protocol when you are connecting to a non-Windows-based server.

To configure these protocols, do the following:

STEP BY STEP

3.9 Configuring Authentication Protocols

1. Open the Routing and Remote Access console.
2. Right-click the server and select Properties. This opens the server properties.
3. Select the Security tab and click Authentication Methods (refer to Figure 3.32). The Authentication Methods dialog box opens (see Figure 3.34).
4. Select the appropriate protocol for a connection and click OK. Click OK to return to the Routing and Remote Access console.

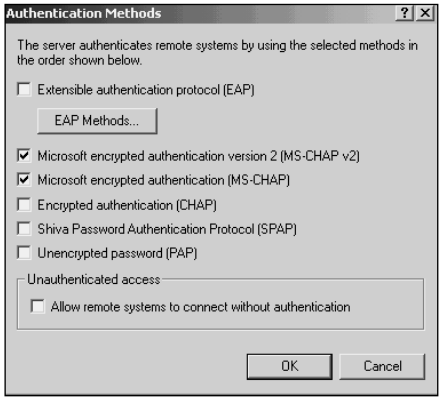
Authentication Methods
The server authenticates remote systems by using the selected methods in the order shown below.
Extensible authentication protocol (EAP)
EAP Methods...
Microsoft encrypted authentication version 2 (MS-CHAP v2)
Microsoft encrypted authentication (MS-CHAP)
Encrypted authentication (CHAP)
Shiva Password Authentication Protocol (SPAP)
Unencrypted password (PAP)
Unauthenticated access
Allow remote systems to connect without authentication
OK
Cancel

FIGURE 3.34
Remote Access security is controlled from this dialog box.

Configuring Encryption Protocols

The first thing you need to be aware of when discussing the encryption protocols available with Windows 2000 is that two main encryption protocols are used in a Windows 2000 VPN. We discussed PPTP and IPSec earlier in the chapter, but a couple of encryption protocols are used in conjunction with IPSec that we need to cover.

06W2000 NITG-03 10/11/00 12:59 PM Page 160

Under the Microsoft model, IPSec encryption does not rely on any authentication methods for its initial encryption keys. The encryption method is determined by the IPSec SA (Security Association). An SA is a combination of a destination address, a security protocol, and a unique identification value, called an SPI (Security Parameters Index). The available encryptions for IPSec include the following:

- **Data Encryption Standard (DES).** DES uses a 56-bit encryption key. This is considered barely adequate encryption for business use, and this level of encryption has been broken using specialized hardware.
- **Triple DES (3DES).** Like DES, 3DES uses a 56-bit key. But as the name implies, it encrypts the data using three 56-bit encryption keys. This is considered to be a 168-bit encryption key ($3 \times 56 = 168$) and is used in high-security environments. Until recently, the U.S. government tightly controlled the export of applications using 3DES encryption. Although these restrictions have been relaxed, exporting 3DES applications still requires government approval.

These are the encryption protocols available for remote access in Windows 2000. Windows 2000 does use other encryption, such as Kerberos, for logging on to a domain, but it is not applicable to remote access. To configure these protocols, do the following:

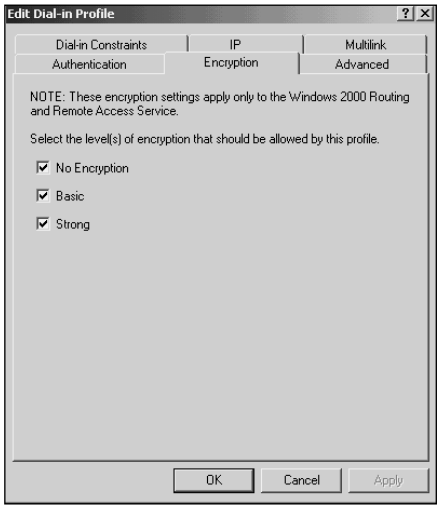

FIGURE 3.35
Windows 2000 supports three levels of encryption.

STEP BY STEP

3.10 Configuring Encryption Protocols

1. Open the Routing and Remote Access console and select Remote Access Policies from the tree view. In the right pane, right-click the policy you want to set the encryption level for and select Properties.
2. From the Policy Properties dialog box, click Edit Profile. The Edit Dial-in Profile dialog box opens.
3. Click the Encryption tab shown in Figure 3.35. You can set the encryption levels to No Encryption, Basic, Strong, or any combination of the three. Select the appropriate level, and then click OK twice and you are back to the Routing and Remote Access console.

06W2000 NITG-03 10/11/00 12:59 PM Page 161

CASE STUDY: IMPLEMENTING ROUTING AND REMOTE ACCESS IN A COMPLEX ENVIRONMENT

ESSENCE OF THE CASE

The essence of the case is as follows:

- The management of your company is reluctant to make a major investment in toll charges for a dial-based remote access solution.
- Your company has three main populations of users, each with different remote access requirements.
- Each team has the requisite level of security.

SCENARIO

You are the network administrator for NR Widgets Inc., a multinational conglomerate, and you are based in the conglomerate's corporate headquarters. NR Widgets Inc. has a mobile population of about 200 people who need access to the network for submitting expense reports.

About 100 of the users live and work within your local area code, and the rest are scattered throughout the country. Your management does not want to pay for long-distance calls for remote access.

Your mobile users consist of three groups. The first group is the highly technical telecommuters, who need access to everything. They are also very security conscious and want to make sure their information is as secure as possible. The second group is the local users who need access, but are not too concerned about the security of the connection. The third group consists of about 35 users who work from home and have high-speed Internet connections.

What is the best way to do this so that you can accomplish the following:

- Each group has access to the network.
- Each group of users has the information security it needs.
- Long-distance or toll-free numbers are not allowed.

What should you do?

continues

06W2000 NITG-03 10/11/00 12:59 PM Page 162

CASE STUDY: IMPLEMENTING ROUTING AND REMOTE ACCESS IN A COMPLEX ENVIRONMENT

continued

ANALYSIS

As you have discovered in this chapter, you can meet these requirements by installing the Windows 2000 Routing and Remote Access Service. But by now you probably realize that it is a bit more complicated than just running the configuration wizard. First you need to take a close look at each population of users. The technical telecommuters, who have access to confidential information, will need to have a configuration that leverages the robust security and encryption mechanisms of the Windows 2000 Routing and Remote Access Service. You may need their profile configure dial-back, and may also need to use smart cards for authentication. For the second group of users, you will probably need to limit their access to sensitive information on the network, since they are using a less secure, more user-friendly authentication policy. Finally, while it is easy to configure a network—for example, an Internet-based VPN, you still need to make decisions. You need to examine the amount of bandwidth you have to the Internet to support these users. You need to consider where the server is placed. Should it be behind a firewall or directly on the Internet? You need to consider which VPN protocol is best suited for your environment. You may even find that your remote users who are not in the local area code want to utilize a local ISP in conjunction with the VPN solution, allowing you to further save on toll charges. All this is very dependent on the environment and the circumstances and requires effective planning. You need to install the following:

- One server running Windows 2000 Server and the Routing and Remote Access Service.
- The server needs to have modems installed and configured for dial-in users.
- Users who do not have the ability to dial locally to the server need to leverage the Windows 2000 VPN service; therefore, the server needs an Internet connection.
- The server needs remote access profiles to control the session security for each group.

This should be fairly straightforward after you have read the chapter. Let's do a quick chapter recap and then move on to some exercises.

06W2000 NITG-03 10/11/00 12:59 PM Page 163

CHAPTER SUMMARY

In this chapter we have covered in detail how to use the Windows 2000 Routing and Remote Access Service to provide remote access services. We started the chapter discussing how to configure Routing and Remote Access to support inbound connections, DHCP, VPNs, multilink connections, and we also discussed the creation and use of a remote access policy. We have examined how to use and configure a remote access profile as well.

We then discussed monitoring and managing the Routing and Remote Access Service and wrapped up the chapter by discussing the different security aspects of the service, including configuring remote access security, authentication protocols, and encryption.

And that wraps up the chapter summary. Let's take a look at some exercises and questions.

KEY TERMS

- virtual private network (VPN)
- modem
- multilink
- encryption
- Dynamic Host Configuration Protocol (DHCP)
- authentication
- Remote Access Service (RAS)
- callback

06W2000 NITG-03 10/11/00 12:59 PM Page 164

APPLY YOUR KNOWLEDGE

Exercises

3.1 Creating a Remote Access Policy

In the following exercise, you will use the Routing and Remote Access console to create a remote access policy. For this exercise you will create a policy for users connecting with PPP.

Estimated Time: 10 minutes

1. Open the Routing and Remote Access console.
2. Expand the application tree in the left pane by double-clicking the server. Right-click Remote Access Policies and select New Remote Access Policy.
3. Enter the name **`Exercise 1`** and click Next to continue.
4. Click Add to add a condition. Select the Framed Protocol attribute from the list of attributes and click Add.
5. Select PPP from the list of protocols. Click Add.
6. Click OK to add the condition. Click Next.
7. Select the Grant Remote Access Permission option. Click Next.
8. Click Finish to complete the creation of the profile.

3.2 Configuring an Idle Timeout for Routing and Remote Access Server

This exercise will walk you through modifying a profile to add an idle timeout for a remote access policy.

Estimated Time: 15 minutes

1. Open the Routing and Remote Access console.
2. Right-click the Exercise 1 remote access policy created in the last exercise. Select Properties from the Context menu.
3. Click the Edit Profile button.
4. Go to the Dial-Constraints tab. Select the Disconnect If Idle option and set the timeout value to 30 minutes.
5. Click OK to commit the changes. Click OK to return to the Routing and Remote Access console.

3.3 Monitoring Routing and Remote Access Using the Performance Console

This exercise will walk you through adding a counter to the Performance console so that you can see how many errors the Routing and Remote Access ports are experiencing.

Estimated Time: 15 minutes.

1. Open the Performance console.
2. In Performance, select System Monitor.
3. Click the Add (+) icon to add the counter.
4. Select the RAS Total performance object.
5. Select the Total Errors counter and click Add.
6. Click Close to complete the exercise.

Review Questions

1. You are the network administrator for Exponent Mathematicians and you have been asked to review the authentication protocols being used by your Routing and Remote Access server. What are the available protocols, and how do they work?

06W2000 NITG-03 10/11/00 12:59 PM Page 165

APPLY YOUR KNOWLEDGE

2. You are the administrator of the Get Stuffed Taxidermists chain Routing and Remote Access server. You have users who are utilizing the Windows 2000 VPN, both with IPSec and PPTP protocols. What are those protocols, and which is the industry standard?
3. You are the Windows 2000 administrator for Bug-B-Gone Exterminators. Your users are all connecting to your network using 56K modems, and they are complaining about performance. You are using the Routing and Remote Access Service with a modem bank for providing access, and they are running Windows 2000 Professional. You have used the performance monitoring capabilities of Windows 2000 to determine that no issues exist with Routing and Remote Access, so the issue appears to be bandwidth limitations. What should you do?
4. You have just installed Routing and Remote Access for providing VPN services to 100 of your end users. You are able to get the first five users connected, but then the server denies access. What is the problem and how do you fix it?
5. You're the LAN administrator for Think About IT Consulting Services company. You have just installed your first Routing and Remote Access server and your users are connecting without a problem. You want to see how much traffic is being added to the network by the additional users. How can you check?

Exam Questions

1. What portion of the Routing and Remote Access Service can be used to aggregate bandwidth across multiple modem connections?

   A. Multinet

   B. Multilink

   C. X.25

   D. VPN

2. You are the system administrator for Phil's Phill-up Stations, a chain of gas stations. As part of the network, you maintain a Windows 2000 Routing and Remote Access server to provide remote access services as part of a VPN. What VPN protocols will the server support?

   A. PPTP

   B. IPSec

   C. PPP

   D. EAP

   E. L2TP

3. You are the LAN Administrator for the OUI Find-em detective agency. You have people connecting to your Windows 2000 Routing and Remote Access from all over the country, most working from home. How can you minimize the users toll charges using Routing and Remote Access?

   A. Configure the user's RAS client computer for Connect as Needed mode.

   B. Use IPSec to tunnel to the RAS server through the public phone network, bypassing the toll charges.

   C. Get each user a personal 800 number.

   D. Set the Routing and Remote Access server security to use callback.

06W2000 NITG-03 10/11/00 12:59 PM Page 166

APPLY YOUR KNOWLEDGE

4. You are the LAN Administrator for Little Faith Enterprises Meat Packing. As part of the troubleshooting of a support issue, you need to check to see whether a user is connected to the Routing and Remote Access server.

   How can you check to see if the user is logged on?

   A. Open Performance Manager. Click the Add Counter icon. Select the RAS object and choose the Connected Users counter. Click OK and check the resulting statistic.

   B. Open the Performance console. Click the Add Counter icon. Select the RAS object and choose the Connected Users counter. Click OK and check the resulting statistic.

   C. Open the Routing and Remote Access console. Right-click the RAS server and choose Connected Users. Check for the user in the Connected Users dialog box.

   D. Open the Routing and Remote Access console. Under the server in the tree view, select Remote Access Clients. Check for the user in the Remote Access Clients.

5. You need to configure strong authentication for your Windows 2000 Routing and Remote Access server. Which protocol(s) should you use?

   A. IPSec

   B. PAP

   C. EAP

   D. CHAP

   E. MS-CHAP

6. You manage a Windows 2000 Routing and Remote Access server used for remote dial-in access. You have an end user who is trying to connect to the Routing and Remote Access server, but he keeps getting the message that he is not an authorized user. He is able to connect to the network and log in from his office across the LAN.

   What might be causing the problem?

   A. The user is not using the correct password.

   B. The user is not using an ID that is authorized to use the dial-in server.

   C. He is trying to use his LAN account instead of his dial-in account.

   D. One of the modems on the server is probably down.

7. You manage a Windows 2000 Routing and Remote Access server used for remote dial-in access. You have an end user who is trying to connect to the Routing and Remote Access server, but keeps getting the message that he is not an authorized user. He is able to connect to the network and login from his office across the LAN. After doing some research you find that the user ID was not authorized for remote access. How would you fix this situation?

   A. Using the Routing and Remote Access console, open the user's ID and under the Remote Access tab, grant him access.

   B. Using the Routing and Remote Access console, create a remote access policy. Use the Windows-Groups criteria and add the user to an authorized group.

   C. Using the Routing and Remote Access, create a remote access profile. Use the Windows-Groups criteria and add the user to an authorized group.

06W2000 NITG-03 10/11/00 12:59 PM Page 167

APPLY YOUR KNOWLEDGE

D. Using the Routing and Remote Access, create a remote access profile. Configure that profile to Grant Remote Access Permission.

8. You are the network administrator for Runaway Travel and you have just installed a new Windows 2000 Routing and Remote Access server to replace a hardware RAS server. Your users are using a third-party PPP dialer that was used for the old system.

   What is the most secure authentication protocol that can be used for this connection?

   A. PAP

   B. EAP

   C. CHAP

   D. IPSec

9. You are the network administrator for Runaway Travel and you have just installed a new Windows 2000 Routing and Remote Access server to replace a hardware RAS server. Your users are using the Windows 2000 Professional dialer.

   What is the most secure authentication protocol available?

   A. CHAP

   B. MS-CHAP

   C. PPP

   D. IPSec

10. You are the network administrator for Runaway Travel and you have just installed a new Windows 2000 Routing and Remote Access server to replace a hardware RAS server. Your users are using a variety of client computer operating systems and PPP dialers.

    What is the most secure way to ensure that all your users have access?

    A. In the dial-in profile for those users, select Microsoft Encrypted Authentication (MS-CHAP) and Microsoft Encrypted Authentication version 2 (MS-CHAP v2).

    B. In the dial-in profile for those users, select Encrypted Authentication (CHAP).

    C. Use IPSec in conjunction with RAS.

    D. Allow remote PPP client computers, as well as all the other protocols, to connect without negotiating any authentication method.

11. You are the network administrator for Go to Philly bus company and you have a requirement for a Windows 2000 Routing and Remote Access server to replace a hardware solution.

    How do you install and configure the service?

    A. Using the Networking and Dial-up Connections Wizard, install the Routing and Remote Access Service.

    B. Using the Networking and Dial-up Connections Wizard, install the Remote Access Service.

    C. Use the Routing and Remote Access Service to configure the service. Configure it with Windows 2000 Administration.

    D. Use the Add/Remove Programs to add the Routing and Remote Access Service to the server. Configure the application using the Routing and Remote Access Service.

06W2000 NITG-03 10/11/00 12:59 PM Page 168

APPLY YOUR KNOWLEDGE

12. You are the system administrator for Blue Cap Haberdashery, and you have a Windows 2000 Routing and Remote Access server acting as a dial-in server. You have 15 modems on the server for users to dial in. Ten users have connected and are able to connect to the network. The eleventh user is able to connect, but cannot reach anything on the network.

    What could the problem be?

    A. The server is licensed for only 10 dial-in users.

    B. The DHCP server was down when the eleventh user tried to connect.

    C. The user has an incompatible modem.

    D. The user's IPSec password is incorrect.

13. You are the system administrator for Blue Cap Haberdashery, and you have a Windows 2000 Routing and Remote Access server acting as a dial-in server. You have 15 modems on the server for users to dial in. Users are able to connect without any problems, but they cannot reach any systems by DNS name. They are able to connect using the IP address of the system.

    What could the problem be?

    A. The Routing and Remote Access server is not running the DNS service.

    B. The Routing and Remote Access server is not running the WINS service.

    C. The network DHCP server has a bad DNS configuration.

    D. The network WINS server has a bad DNS configuration.

14. You are the security administrator for Barb's House of Pancakes. You have been asked to implement smart cards for remote access authentication using the Windows 2000 Routing and Remote Access Service.

    What protocol do you need?

    A. IPSec

    B. PPTP

    C. MS-CHAP v2

    D. EAP

15. You are the network administrator for Phil 'Em Up gas stations. You have installed a Windows 2000 Routing and Remote Access server to provide access to the corporate network remotely. You want to see what kind of utilization the server is experiencing.

    What is the easiest way to find out?

    A. Use Performance Manager to log the utilization. Check the performance logs for the information.

    B. Use the Performance console to log the utilization. Check the performance logs for the information.

    C. Go into the Registry and enable logging. Check the log file for the information.

    D. Go to the Event Logging tab in the Routing and Remote Access Server properties. Check the application log using the Event Viewer application to view the statistics.

16. You are the network administrator for Ye of Little Faith advertising, and you are running a Windows 2000 network made up of six Windows 2000

06W2000 NITG-03 10/11/00 12:59 PM Page 169

APPLY YOUR KNOWLEDGE

servers and 300 Windows 2000 Professional client computers. You have added 30 modems to the backup domain controller and need to install and configure the server for inbound connections. A secondary objective would be to install and configure VPN services.

You do the following:

Open the Networking and Dial-up Properties and double-click the Make New Connection icon. You follow the wizard to complete the installation, selecting Allow Virtual Private Connections to ensure that your VPN works.

This solution:

A. Is functional and meets the primary and secondary objectives.

B. Is functional but meets only the primary objective.

C. Is functional but meets only the secondary objective.

D. Is not functional.

17. You are the system administrator for Run to the Hills Travel. You have a Windows 2000 Routing and Remote Access server configured to use multilink. You would like to configure the server to automatically drop a connection when the lines are not being used.

    What protocol can you use to accomplish this?

    A. PPP

    B. BAP

    C. PPTP

    D. EAP

18. You are the Internet administrator and you are using Windows 2000 Server as a VPN server. You need to configure additional IPSec VPN ports.

    How do you accomplish this?

    A. Run the VPN wizard and configure the additional ports.

    B. Go to the Networking and Dial-up Connections window and double-click New Connection. When the New Connection wizard starts, select New Inbound VPN and follow the prompts.

    C. In the Routing and Remote Access console, edit the properties of the L2TP ports and add the additional connections.

    D. In the Routing and Remote Access console, edit the properties of the IPSec ports and add the additional connections.

19. You are the security administrator for a small police force. Your network is based on Windows 2000 Server, and you have just purchased smart cards for the entire force. You would like to take advantage of these for remote access, but you are unsure how to configure Routing and Remote Access. You know you need the EAP protocol.

    Where do you configure this protocol?

    A. In the remote access policy.

    B. In the modem pool properties.

    C. Under the Security tab of the Routing and Remote Access server properties.

    D. In the dial-in profile for the pertinent policy.

06W2000 NITG-03 10/11/00 12:59 PM Page 170

APPLY YOUR KNOWLEDGE

20. What is the strongest encryption protocol supported by Windows 2000?

    A. DES

    B. IPSec

    C. MS-CHAP v2

    D. 3DES

21. You are the security administrator for Jolly Snowmen Ice Cream. You have been asked by your manager to explain the use of encryption on your Windows 2000 server. You know you are running DES.

    What service does DES provide to your installation?

    A. DES encrypts dial-in traffic over the phone lines.

    B. DES encrypts L2TP VPN traffic.

    C. DES provides encrypted authentication.

    D. DES provides encrypted address information in conjunction with PPTP.

Answers to Review Questions

1. The authentication protocols available include the following:

   - **EAP-TLS.** The Extensible Authentication Protocol (EAP) is an extension to the Point-to-Point Protocol (PPP). EAP provides a standard mechanism for support of additional authentication methods within PPP, such as smart cards, one-time passwords, and certificates. EAP is critical for secure Windows 2000 VPNs because it offers stronger authentication methods (such as X.509 certificates) instead of relying on the user ID and password schemes used traditionally.
   - **CHAP.** The Challenge Handshake Authentication Protocol (CHAP) negotiates an encrypted authentication using MD5 (Message Digest 5), an industry-standard hashing scheme. CHAP uses challenge-response with one-way MD5 hashing on the response. This allows you to authenticate to the server without actually sending your password over the network. Because this is an industry-standard authentication method, it allows Windows 2000 to securely connect to almost all third-party PPP servers.
   - **MS-CHAP.** Microsoft created Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), an extension of CHAP, to authenticate remote Windows workstations, increasing the protocol's functionality by integrating the encryption and hashing algorithms used on Windows networks. Like CHAP, MS-CHAP uses a challenge-response mechanism with one-way encryption on the response. Although MS-CHAP is consistent with standard CHAP as much as possible, the MS-CHAP response packet is in a format specifically designed for computers running a Windows operating system. A new version of the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP v2) is also available. This new protocol provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving.

06W2000 NITG-03 10/11/00 12:59 PM Page 171

APPLY YOUR KNOWLEDGE

- **SPAP.** Shiva Password Authentication Protocol (SPAP) is used specifically to allow Shiva client computers to connect to a Windows 2000 Server and to allow Windows 2000 client computers to connect to Shiva servers.
- **PAP.** Password Authentication Protocol (PAP) uses unencrypted (plain text) passwords for authenticating users and is considered the least secure authentication protocol available. PAP is usually used as the authentication of last resort—used when a more secure form of authentication is not available. You might need to use this protocol when you are connecting to a non-Windows-based server.

2. Understanding the differences between IPSec and PPTP is important. These points should help you distinguish between the two:
   - **IPSec (IP Security Protocol).** IPSec is a suite of cryptography-based protection services and security protocols used to provide a secure VPN connection. IPSec provides machine-level authentication, as well as data encryption, for L2TP-based (Layer 2 Tunneling Protocol) VPN connections. Unlike some other IPSec-based VPNs, Microsoft's implementation uses the L2TP protocol for encrypting the usernames, passwords, and data, whereas IPSec is used to negotiate the secure connection between your computer and its remote tunnel server. All authentication under the Microsoft IPSec VPN occurs through L2TP connections. These use all standard PPP-based authentication protocols to authenticate the user after the secure IPSec communication is established.
   - **PPTP (Point-to-Point Tunneling Protocol).** PPTP is Microsoft's legacy protocol for supporting VPNs. Developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known collectively as the PPTP Forum, PPTP encountered some security issues in its original form. It has been revised by Microsoft, but it has never been widely accepted by the security community. Although still supported on a variety of vendors' VPN servers, PPTP is rapidly being overtaken by the more widely adopted IPSec protocol.
3. The only way to provide additional bandwidth short of a different access media is to enable multilink and have the users add an additional modem and modem line on the remote end. This will allow the users to aggregate their bandwidth across two separate connections.
4. By default, Routing and Remote Access is configured with five connections for the VPN. You need to open the Routing and Remote Access application and go into the Port properties. Add additional ports as needed.
5. To find out the raw numbers on bandwidth through the server, you need to use the Performance console. Go to the RAS Total object and add the Total Bytes Received and Total Bytes Transmitted counters. Add the two counters to get the total additional traffic.

06W2000 NITG-03 10/11/00 12:59 PM Page 172

APPLY YOUR KNOWLEDGE

Answers to Exam Questions

1. **B.** The correct term for this feature is multilink. See "Configuring Multilink Connections."
2. **A, B, E.** The Windows 2000 Routing and Remote Access will support the following VPN protocols: IPSec, PPTP, and L2TP. See "Configuring a Virtual Private Network (VPN)."
3. **D.** If you configure the Routing and Remote Access server to use callback, all the toll charges following the initial connection will be on the company's bill, not the end user's. This is an old trick for reducing costs by leveraging the company's generally more favorable long distance rates. See "Configuring a Remote Access Profile."
4. **D.** You can see this information in the right pane of the Routing and Remote Access console by clicking the Remote Access Clients entry. See "Configuring Authentication Protocols."
5. **C, D, E.** IPSec is not an authentication protocol. PAP sends the authentication information as clear text. EAP, CHAP, and MS-CHAP are all secure authentication protocols. See "Creating a Remote Access Policy."
6. **B.** The user is not using an ID that is authorized to use the dial-in server. You must be authorized in a remote access policy before you can connect via dial-in. See "Creating a Remote Access Policy."
7. **B.** Using the Routing and Remote Access console, create a remote access policy. Use the Windows-Groups criteria and add the user to an authorized group. See "Creating a Remote Access Policy."
8. **C.** With a third-party dialer, the best you will be able to manage for authentication is the CHAP protocol. CHAP is an industry-standard protocol supported by virtually all PPP dialers. PAP would also work, but offers no security whatsoever. IPSec is not an authentication protocol. EAP is a protocol used for devices such as smart cards. See "Configuring Authentication Protocols."
9. **B.** When you are communicating between Windows PPP client computers, MS-CHAP is the most secure protocol listed. See "Configuring Authentication Protocols."
10. **D.** The trick here is to understand that the "connect without negotiating any authentication method" configuration is the lowest common denominator for connections. That's the only way to ensure that all your users can get to the network using your RAS solution. Users can still connect using greater security. See "Configuring Authentication Protocols."
11. **C.** The Routing and Remote Access Service is installed with the operating system. You will need the Routing and Remote Access console to make sure everything is configured correctly. See "Configuring Inbound Connections."
12. **B.** The Routing and Remote Access Service will request 10 addresses from the network DHCP server when it starts. When those 10 have been issued, RRAS will request an additional 10 addresses. If the DHCP server has gone down since the original 10 addresses were issued, the user would be able to connect but would not be able to get on the network because the Routing and Remote Access Service couldn't get additional IP addresses from the DHCP server. See "Configuring Routing and Remote Access for DHCP Integration."

06W2000 NITG-03 10/11/00 12:59 PM Page 173

APPLY YOUR KNOWLEDGE

13. **C.** Because the Routing and Remote Access server gets its DHCP information from the network DHCP server, a bad DNS configuration on the DHCP server could cause the issue described. See "Configuring Routing and Remote Access for DHCP Integration."

14. **D.** EAP is the protocol needed to support smart cards. See "Configuring Authentication Protocols."

15. **D.** In the latest version of Routing and Remote Access, logging is enabled in the server properties. The results of the logging can be found in the Event Viewer. See "Managing and Monitoring Remote Access."

16. **D.** This solution will not work because you must use the Routing and Remote Access console to configure remote access on a domain controller. See "Configuring Inbound Connections."

17. **B.** BAP (Bandwidth Access Protocol) is used to accomplish this function in conjunction with multilink. See "Configuring Multilink Connections."

18. **C.** You can just edit the properties of the L2TP ports, which are installed and configured when Routing and Remote Access is installed. Because by default IPSec used L2TP as a transport under Windows 2000, the ports are L2TP ports, not IPSec ports. See "Configuring a Virtual Private Network (VPN)."

19. **D.** The authentication protocols are configured in the dial-in profile. Although A is almost right, this is not configured as part of the policy, but is instead part of the profile. See "Configuring a Remote Access Profile."

20. **D.** 3DES or Triple DES is the strongest encryption protocol used by Windows 2000. See "Configuring Encryption Protocols."

21. **B.** DES is used in conjunction with IPSec. Because IPSec is used with L2TP, B is the correct answer. See "Configuring Encryption Protocols."

Suggested Readings and Resources

1. Boswell, William. *Inside Windows 2000 Server.* Indianapolis, IN: New Riders Publishing, 2000.

2. Siyan, Karanjit S. *Windows NT TCP/IP.* Indianapolis, IN: New Riders Publishing, 1998.

06W2000 NITG-03 10/11/00 12:59 PM Page 174